

Appendix N— Privacy & Security Framework: Safeguards Domain

1 Introduction

The purpose of this document is to provide guidance from the perspective of Nevada’s Director of the Department of Health and Human Services (DHHS Director), who is also the designated State Health IT Authority (NRS 439.587), regarding the proper safeguards in the electronic handling and sharing of protected health information (PHI), individually identifiable health information (IIHI) and electronic health record (EHR) data. The document will establish a baseline understanding of and requirements for the Safeguard Standards set forth in the HIPAA Security Rule. It is NHIE’s intent to model its data sharing functionality after these standards, and require all NHIE Covered Entities and participants to do the same.

In addition to directing NHIE participants to functionally and procedurally comply with these standards for handling an individual’s PHI, the Director also has a number of State specific statutes in place for the Nevada Health Information Exchange. These policies will be further detailed and developed by the State with the full NHIE governance, technology, procedures, and policies platform by mid 2013. In addition, State regulations will be required and are expected to be developed collaboratively with the health community during 2013 and passed by State Legislature by mid 2014.

Implementation of the guidelines and requirements set forth in this document will be a function of the HIE infrastructure that NHIE will procure or subscribe to in early 2013.

2 NHIE User Authorization and Authentication

While the specific technology platforms for HIE may differ across vendor solutions, user authorization and authentication processes will perform similarly.

As the NHIE begins, and as it evolves, core privacy and security functionality must remain consistent across HIE platforms and solutions over time. In order to drive this continuity in core function, NHIE will be using recommendations set forth by the ONC Privacy and Security Tiger Team as guidance for ongoing functionality of user authorization and authentication. ONC Tiger Team recommendations have been updated as recently as August 2012. Also, by incorporating Tiger Team recommendations into NHIE functionality, this can help ensure ongoing compliance with ONC directives, and compatibility with other HIEs and NWHIN networks as services and functions must integrate and interconnect.

Starting With a Solid Identity Management Foundation

The cornerstone of HIE systemic access and trust is capability to verify that a person, entity, or process:

- is who or what they claim to be, and
- that they have verifiable reason, authenticated privileges, and an authorized relationship to patients and patient data exposed within the NHIE network.

The essential system tool or application to identify, authorize, and authenticate users to the NHIE will be deployment of an enterprise master person/patient index (EMPI), or what is also known as a master data management (MDM) application. The latter indicates that the identity, authorization, and authentication functionalities go beyond just the patient aspects of this process to include caregivers/doctors and other providers, entities, and processes.

The task of an EMPI/MDM specifically to healthcare, is to control valid access to the NHIE based on patient consent choice, validated identity, , and established relationships between users, the data, and the participating systems. The EMPI/MDM will further identify, match, merge, de-duplicate, and cleanse patient, person, and entity records to create a master index that may be used to obtain a complete and single view of a patient based on the privileges to do so.

2.1.1 Authorization and Authentication Control

Who controls the authorization and authentication processes for access to and use of information within the NHIE, and at what level(s) of assurance (LOA)? Controls on identity within NHIE and access to patient information shared across the network will be organized in a tiered manner. That is to say that levels of user identity, assurance, and their organizational affiliation will be defined and controlled by an overall NHIE EMPI/MDM administrator. This process will adhere to LOA guidelines as recommended by the ONC Privacy and Security Tiger Team.

NHIE User Authorization and Authentication Oversight and Control

At each user level, the overall NHIE EMPI/MDM Administrator will maintain review and approval status for all users and entities defined within the EMPI/MDM system. There will (likely) be three primary points of individual registry control into the system, and will (likely) look as follows;

1. End User (person, process) → 2. Organization Super-User → 3. NHIE EMPI/MDM Administrator

Level(s) of Assurance for NHIE User Authorization and Authentication

It is expected that user access to the NHIE will be granted from any number of locations, device types, and internet portals. This access can originate from within a closed system (ie.from within other HIEs or healthcare systems with access options to NHIE), public and private workstations and laptops, and handheld (cellular/mobile) smart devices. Access to NHIE may be needed by a qualified and authorized participant from within the state, or from anywhere a viable internet connection to the NHIE is available. Physical location may not be a constraining factor.

LOAs can be defined on four levels, and NHIE will follow the established NIST (National Institute of Standards and Technology) guidelines for LOA. Additionally, due to the expected diversity in users, user types, and the varied points and types of NHIE access, NHIE intends to follow, at minimum, LOA(3).

As in other technical aspects of NHIE, following the ONC Tiger Team Recommendations and NIST guidelines for LOA will a high level of operational security and confidence and help ensure NHIE compatibility with other HIEs and NWHIN networks. And though at the time of this writing the NHIE and its Governance and

Operational organization have not yet selected a HIE technology vendor, whatever vendor solution is chosen will be required to be compliant with NHIE's LOA requirements.

LOAs can be generally defined as follows:

LOA(1)	Provides little or no confidence in the asserted identity's authorization and authentication.
LOA(2)	Provides some confidence in the asserted identity's authorization and authentication.
LOA(3)	Provides high confidence in the asserted identity's authorization and authentication.
LOA(4)	Provides very high confidence in the asserted identity's authorization and authentication.

2.1.2 Mapping Users Across Multiple Entities Within the NHIE

How is one NHIE user mapped from one participating organization to one or more other NHIE participating organizations? When considering all users of an HIE, it is likely that care givers, from doctors to nurses to specialists and others, may hold multiple roles within an organization, and may hold positions (possibly with multiple roles) at multiple participating organizations within the NHIE. It is vital to the privacy and security of the NHIE and trust within the network that the HIE platform recognizes these conditions. The HIE must recognize the person/user at the moment, positively identify, authorize, and authenticate that person on the system – and at the same time recognize and validate that person's organizational affiliation at the time of and for the duration of the HIE session. Generally speaking, the EMPI/MDM functionality (either as an add-on application or integral native functionality to the HIE solution) will be the primary functionality that monitors and manages this situation. This includes maintaining a person's authorized relationship to specific NHIE patient information based on that person's identity, their organizational affiliation/ association at the time of and duration of the HIE session, and the patient's consent stipulations which apply to that person/user and organization at the time of the HIE session.

HIE User Organizational Mapping Matrix

Regardless of the EMPI/MDM solution eventually deployed for NHIE, the data elements that make up a user definition and organization affiliation matrix are likely very similar from solution to solution. A basic user profile will be established. This profile can have multiple iterations of roles for a single organization, and there may be multiple iterations of organizational affiliations for a single person. All of the relational aspects of this situation must be managed and monitored accordingly.

For example, a doctor may work for hospital-A. While working for hospital-A, one of this doctor's roles may be as a resident with house privileges to visit and treat patients as needed. This same doctor may also have an occasional or regular role as an ER doctor, where such user security privileges as break-the-glass may apply to this doctor - where such ER authorization(s) would not apply to this doctor in his or her role as a resident performing routine rounds. The systemic relationships here must be maintained by person, by location, by time, by patient relationships, and potentially other factors. So, for example, when a doctor has ER privileges with break-the-glass authorizations, those authorizations can only be granted to the user when physically in the ER, and not carry over to his or her role when they are logged into the system as a resident.

This broad user picture and definition within the HIE can be iterative. This takes into account the affiliation of a user's role and responsibilities at multiple organizations throughout the HIE. Therefore, it is essential that the NHIE work closely with individuals and their affiliated organizations so that the NHIE EMPI/MDM Administrator can see to it that the user's NHIE profile is defined correctly. And, within this process, each and every user/organization relationship, with roles and authorizations, etc, must be set up correctly as well.

This process must also account for monitoring when a user's privileges at an organization change, are restricted, constrained, or prohibited, so that use of the HIE does not inadvertently allow unauthorized or otherwise expired access to the NHIE network for one or more individual affiliations.

From a technical perspective, NHIE expects to employ best practices for such open standards as SOA (Service Oriented Architecture), SSO (Single Sign On), and CCOW (Clinical Context Object Workgroups) when designing, defining, and deploying this functionality.

2.1.3 Nevada as an Opt-In State

How does a patient Opt-In model for state HIE promote proper and Authorized use of PHI? In 2011, the state of Nevada passed Senate Bill 43 (SB 43) which specifically deals with aspects of ehealth and health information exchange. It also addresses issues specific to patient privacy and choice with regard to a patient participating in the state's health information exchange, and the patient granting (or denying) permission to have their health records transmitted by electronic means of any type. By requiring this approach, Nevada is promoting and encouraging patient/physician relationships, informed patient consent, and patient choice (and the individual-choice domain of PIN-003).

The following is an excerpt from SB43:

Sec. 11. 1. Except as otherwise provided in subsection 2 of NRS 439.538, a patient must not be required to participate in a health information exchange. Before a patient's health care records may be transmitted electronically or included in a health information exchange, the patient must be fully informed and consent, in the manner prescribed by the Director, to the transmittal or inclusion. (from page 8 of SB 43)

2.2 Identified vs De-identified Patient Information

Why is there a distinction between and need for identified and de-identified patient information? Under the HIPAA privacy rule, there are specific patient data that are protected from use outside of the patient's immediate continuum of care. However, there are also guidelines for use of patient data for general research, analytics, etc, whereby care information can be shared for such purposes as long as the data cannot be linked or attributed to any specific individual (patient).

There are many factors which impact identified (identifiable) information and de-identified information as set forth in HIPAA (45 CFR). At a high level, however, it is essential to all users and custodians/stewards of patient data to understand 4 major concepts, descriptions, and guidelines when dealing with an individual's protected health information (PHI). These 4 major points include Identifies Patient Data, De-identified Patient Data, Individually Identifiable Health Information, and Limited Data Set. Familiarity with these points and associated

references within the HIPAA Privacy Rule is essential to NHIE's proper handling of PHI and maintaining HIPAA compliant procedures and operations.

2.2.1 Identified Patient Data

By HIPAA definition, protected information is generally described as any information or data that is "directly identifiable" to a patient. This includes any single data element or combination of specific data elements within a patient record instance that could determine, directly or indirectly, a patient's identity. The HIPAA privacy rule cites 18 data points - of the individual, and/or his or her relatives, household members, or employers – which could be used alone or in any combination that could deem patient information identifiable. These 18 points include:

1. names,
2. geographic subdivisions smaller than a state (including zip code),
3. all elements of dates except year (unless the subject is greater than 89 years old),
4. telephone numbers,
5. FAX numbers,
6. email address,
7. Social Security numbers,
8. medical record numbers,
9. health plan beneficiary numbers,
10. account numbers of any kind,
11. certificate/license numbers (driver's license, etc),
12. vehicle identifiers (including license plates),
13. device identifiers and serial numbers,
14. URLs,
15. internet protocol addresses,
16. biometric identifiers (including finger prints),
17. full face photos and comparable images, and
18. any unique identifying number, characteristic or code

2.2.2 De-Identified Patient Data

By HIPAA definition, data are considered to be de-identified if the following 2 general conditions are satisfied:

1. An experienced expert determines that the risk that certain information could be used to identify an individual is "very small" and documents and justifies the determination.
2. Data do not include any of the eighteen data points (identifiers) as described above in Identified Patient Data.

Additionally, it is important to note that even if patient data has been scrubbed of any and all identifiable information, including the 18 points cited above, the Privacy Rule states that information will still be considered identifiable if the covered entity knows that the identity of the person may still be determined.

2.2.3 Individually Identifiable Health Information

To understand what data can make up IHII and how IHII determines the proper ownership and use of patient information, it is essential that the distinction between identified patient information and de-identified patient information is clear. HIPAA defines IHII as any individual data element, combination of data elements,

or subset of health information that identifies an individual, or can reasonably be used to determine the identify of an individual.

2.2.4 Limited Data Set

The concept of Limited Data Set (LDS) is significant with regards to properly authorized ownership and use of PHI. The LDS includes the use of de-identified data for research, public health, health care operations, etc, and does not require an authorization/waiver of authorization from the patient. However, request for and use of the LDS will likely require a formal Data Use Agreement between the recipient of the LDS and the Covered Entity. The LDS is defined as PHI that can only include de-identified data as cited above. Though the LDS is subject to only select provisions of the HIPAA Privacy Rule, there may be conditions where it is covered by the “Common Rule” (aka “45 CFR 46”).

The Common Rule outlines requirements of federally supported research with regards to human subject’s protections. The responsibility of these protections is charged to the institutions using the LDS, their Institutional Review Boards (IRBs), and investigators. It also mandates that all researchers obtain informed consent from human patient subjects to participate in research, unless the IRB has approved a waiver of the requirement for informed consent. All research, not just federally supported studies, requires compliance with the Common Rule. The impact here for NHIE could be that any state sponsored public health studies, for example, would require compliance to the Common Rule if including LDS.

2.3 Corrections and Corrective Action

Why must there be solid guidance for corrections and corrective actions in the event of any data and information issues that may occur within the HIE? HIPAA and the HITECH Act set forth directives on maintaining the accuracy and integrity of all processes and data that within an EDI environment. This section deals with corrections and corrective actions to inaccuracies to PH/IIHI. Data breach is covered in another document.

In the event that issues with handling patient health data (PHI/IIHI) do occur, appropriate mitigation and resolution procedures need to be in place by the NHIE. If data, for whatever reason, becomes incorrect or inaccurate, the NHIE must take steps to correct or amend the data as quickly as possible. In most all cases, both the Covered Entity and the Business Associate will be actively involved in any corrective/amendment action procedures.

2.3.1 What Constitutes a correction?

Corrections to PHI/IIHI are warranted when inaccuracies are observed by any authorized person or entity working in the health information exchange network. Additionally, the patient or individual to whom the PHI/IIHI belongs can also report inaccuracies for correction - or - request changes and/or updates to the information contained within their PHI/IIHI or other electronic health record(s).

2.3.2 The Correction Principle

The Correction Principle is spelled out formally in the HIPAA Privacy and Security Framework, CFR 45, section 164.526. Here, the Correction Principle is briefly summarized for purposes of its application to NHIE and the state wide HIE network.

In the event that inaccuracies are noted by authorized persons or entities (including those workforce individuals within a Covered Entity or Business Associate), the following steps should be taken:

- There is an obligation to notify the individual that there is an inaccuracy in their PHI/IIHI/EMR;
- If the correction requires no input from the individual who is the subject of the PHI/IIHI/EMR, then the correction can be made and the individual notified of the update to their electronic health record(s).

In the event that inaccuracies are noted by the individual who is the subject of the PHI/IIHI/EM, the Individuals should be provided with a clear point of contact and timely means to:

1. Dispute the accuracy or integrity of information within their PHI, IIHI, and EMR, and
2. Have erroneous information corrected or to have a dispute documented if their requests are denied.

In this case of providing a clear path to reporting and requesting corrections by the individual or consumer, the consumer can approach either the Covered Entity (which will likely be their doctor or hospital) or the Business Associate (which in this case can include NHIE). The NHIE will have a consumer complaint process in place where requests for corrections to the consumer's PHI/IIHI/EMR can be received, corrected, documented, and the resolution reported back to the consumer to close the process. Depending on the nature of the inaccuracy and the expected correction, it is likely that the NHIE (as the Business Associate) will take the lead on any corrections, but will engage any affected Covered Entity where the consumer's information originated and/or is otherwise stored.

2.3.3 Corrective Action

The HIPAA Privacy Rule defines an individual's right to have their PHI, IIHI, EMR and other health information on the HIE network corrected in a manner consistent with the Correction Principle in the HIPAA Privacy and Security Framework (45 CFR 164.526). The entire process of correcting the consumer's erroneous or inaccurate information should adhere to the following general guidelines:

- Apply the guidelines of the Privacy Rule and the Correction Principle
- The processes, follow-up, and documentation employed by the Covered Entity or Business Associate, must recognize that;
- The consumer has critical and ongoing stake in verifying the accuracy of their electronic medical record(s), and
- They play an active role in ensuring the ongoing integrity of that data.

Per the Privacy Rule, a Covered Entity is obligated to amend/change a consumer's PHI/IIHI/EMR (as defined in 45 CFR 164.501).for as long as that Covered Entity maintains those records. The Covered Entity's responsibilities in this regard are:

- Correct the record as requested by the consumer within 60 days.
- Notify the consumer that their change request is denied, and the reasons for the denial, within 60 days. If the consumer disputes the Covered Entity's denial, the Covered Entity must:
 - Provide the consumer an opportunity to file a statement of disagreement, and

- Provide documentation of the dispute with any subsequent use and/or sharing of that consumer's affected PHI/IIHI/EMR information.
- Notify any and all known Business Associates who also hold that consumers electronic health information that there has been an amendment/correction and make that updated consumer PHI/IIHI/EMR data available to them.

Taking Advantage of NHIE to Expedite Corrective Action

As NHIE is providing a state-wide network for sharing and exchanging health information, it facilitates participating Covered Entities, Business Associates, and Consumers an electronic means for taking corrective actions, resolving issues, and appropriate follow up in a timely, expedient manner. For example, where the Privacy Rule stipulates that changes be affected within 60 days, by using the NHIE network these changes can possibly be resolved in a much shorter time frame.

The Privacy Rule addresses the following written exchanges:

- The individual's request for an amendment,
- The covered entity's notice to the individual that the amendment has been accepted or,
- If denied, the reasons for denial,
- The individual's statement of disagreement,
- The covered entity's rebuttal statement, if any, and
- The notification of other Covered Entities and/or Business Associates known to hold the data that is the subject of the correction.

However, the Privacy Rule also allows the Covered Entity, Business Associate, and Consumer to agree to conduct any of these written exchanges electronically. Thus, when corrective action can be transacted electronically, it is likely that the entire process will be expedited.

2.3.4 In a HIE the Covered Entity and Business Associate Can Be Responsible for Corrective Action

The HIPAA Privacy Rule designates a Covered Entity as the responsible party for acting on an amendment request. However, a HIE as a Business Associate to the Covered Entity, may be required under its Business Associate Agreement (BAA) to perform certain functions related to corrections, changes, and amendments. This could include informing other HIE participants of the amendment. See 45 CFR 164.504(e)(2)(i)(F).

2.3.5 In a HIE the Covered Entity and Business Associate Can Be Responsible for Notification of Corrective Action

Under the HIPAA Privacy Rule, a Covered Entity must make reasonable efforts to:

- Communicate the PHI/IIHI/EMR amendment to others in the HIE network to other parties that are known to have the information about the consumer, and
- Communicate the PHI/IIHI/EMR amendment to others on the HIE network as specifically identified by the consumer, and
- To communicate the amendment within a reasonable timeframe.

However, as the HIE has the ability to track where and with whom information was exchanged in the past, or to otherwise identify what single or multiple locations on the HIE network where the Consumer's

PHI/IIHI/EMR resides, the HIE can assist the Covered Entity as its Business Associate, in efficiently disseminating amended information to appropriate recipients throughout the HIE network.

2.4 Openness and Transparency

Why is openness and transparency with regards to policies and processes in the use of PHI/IIHI/EMR, particularly within an HIE, important for consumers, Covered Entities, Business Associates, and all HIE stakeholders? As stated in the 'Openness and Transparency Principle':

“... There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information...”

This principle impacts and compels all HIE participants, by their roles and responsibilities within the HIE, to be open, transparent, and to that end at the service of the Consumer who's PHI/IIHI/EMR information is being shared and exchanged across the state-wide NHIE network. As partners in serving the needs of the consumer (patient), the State and all NHIE participants will contribute to these policies as well as setting examples in executing their collective openness and transparency efforts within the HIE. This builds a level of integrity, adoption, and trust amongst the HIE participants, but most importantly builds and maintains a level of integrity, adoption and trust in the HIE, its participants, and the information and services provided by the HIE with the Consumer.

Additionally, Nevada Senate Bill 43 (SB 43) was signed into law in 2011 in direct support of the State's HIE/HIT initiatives. Among other provisions of SB 43 that addresses openness and transparency, any state level meetings, for example, must follow the State's 'Open Meeting Law'. This law requires the NHIE – in this example – to conduct all of its business in compliance with Nevada Open Meeting Law (NRS 241), and encourages other NHIE participant organizations throughout the state to conduct their HIE business in an appropriately similar manner.

2.4.1 Openness and Transparency and the HIPAA Privacy Rule

As Nevada deploys its NHIE network and those technologies and services evolve over time, it is essential that trust in its information and use is established amongst all its users. This will ultimately result in ease of use and sharing of PHI/IIHI/EMR information, and improve the quality and timeliness of care delivery. Openness and transparency in all aspects of the use of HIE for sharing and exchanging consumer health data will provide the foundation for this trust, adoption, and improved quality and timeliness of care – and this concept is emphasized in the Openness and Transparency Principle in the Privacy and Security Framework. It also stresses consumer awareness and understanding as to what PHI/IIHI/EMR data exists about them on the HIE.

The consumer should know:

- How and by whom this information is collected
- How and by whom this information is used
- How, why and by whom this information can be disclosed, and

- What reasonable and informed choices can be exercised with respect to that information.

2.4.2 Privacy Rule Notice of Privacy Practice

This guidance addresses the Privacy Rule's notice of privacy practices (NPP) provision and how this Privacy Rule requirement applies to and supports openness and transparency in a HIE. Further, NPP guidelines go on to discuss other functions that occur within a HIE that have impact on HIE applications and the processes they perform.

The Privacy Rule stipulates that the Consumer has the right to receive a copy of the NPP. It requires that the Covered Entity writes the NPP in "plain language" so it is as easy to understand as possible for the consumer (see 45 CFR 164.520). Minimally, the NPP should:

- Describe a Covered Entity's use of The Consumer's PHI and how it is disclosed,
- The Consumer's rights with respect to that information, as well as
- The covered entity's obligations to protect the information.

The Covered Entity should further:

- Provide a copy of the NPP directly to the Consumer on that Consumer's first date of service,
- make a good faith effort to obtain the Consumer's written acknowledgment of receipt of the NPP, and
- Post the NPP at its facility and have it available for anyone requesting a copy.

Relative to a Covered Entity operating in an electronic environment, the Privacy Rule also contains a number of NPP provisions, including:

- The Covered Entity must maintain a website describing its services and will also prominently post its NPP,
- Where a health care provider delivers its *first* health care service to an individual electronically (ie e-mail, any Consumer interaction or communication via internet), the provider must send a NPP (electronically) automatically and contemporaneously in response to the Consumer's request for service.
 - In general, a Covered Entity is also permitted to e-mail the NPP to a Consumer if that Consumer agrees to receive an electronic NPP. However, the Consumer (always) retains the right to receive a paper copy of the NPP upon request (see 45 CFR 164.520(c)(3)).
- The HIE organization as a Business Associate to the Covered Entity is not obligated to provide a NPP to Consumers.
- The Covered Entity may also want to consider adding a description of its participation in the to the content of its explaining its participation in the HIE, the benefits to the Consumer, and general assurance that the Consumer's PHI/IIHI/EMR information is protected, private, and secure.

2.5 Administrative, Physical, and Technical Safeguards

What aspects of HIE and PHI/IIHI/EMR are impacted by administrative, physical, and technical Safeguards? Each of these three major areas impact the overall security program of a Covered Entity within the NHIE, and can directly impact the security characteristics of the hosting HIE in the role of Business Associate. These safeguards offer benefit to Consumers, Covered Entities, and Business Associates within their own interests.

But, these security points also provide assurances within the NHIE network of trust that each participant in the NHIE can depend on the data trading and data use partners within the NHIE to uphold at least minimum standards of secure operations and data integrity. Nevada DHHS through its Governance and Operational organization and NHIE will require that the NHIE participants and Covered Entities comply with these safeguards.

2.5.1 Administrative Safeguards

Administrative safeguards are recommended policies and procedures (found in the Security Rule, 45 CFR Section 164.308) to assure the protection of all PHI/IIHI/EMR information that is processed and shared by a Covered Entity. Although the Covered Entity is the primary organization in this scenario, the Covered Entity's workforce and other trading partners are implicated and impacted as well. This means that the HIE as a Business Associate to the Covered Entity must take steps along the same lines to protect the information it handles. The Security Rule discusses and defines Administrative Safeguards as follows;

“Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the Covered Entity's workforce in relation to the protection of that information.”

The expectation for a Covered Entity and its affected data trading partners will take appropriate steps to assess their current safeguards readiness and capabilities and put a plan in place to address these safeguards. Efforts here could include;

- Inventory and evaluation of security controls already in place.
- Accurate and thorough risk analysis of the processes and procedures involved in handling and protecting PHI/IIHI/EMR data.
- Documented solutions addressing the Covered Entity's major points of safeguards and security.

Administrative Safeguards comprise over half of the HIPAA security requirements. However, these guidelines are not intended to be a definitive set of rules for a Covered Entity's (and their partners) compliance, as the Covered Entity's actual compliance with the Security Rule depend on a number of factors*, including those found in 45 CFR Section 164.306(b)(2);

- (i) The size, complexity, and capabilities of the covered entity.
- (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
- (iii) The costs of security measures.
- (iv) The probability and criticality of potential risks to EPHI (Electronic Protected Health Information).

The Security Management Process - 45 CFR Section 164.308(a)(1)

The Security Management Process standard describes processes and procedures that the Covered Entity (and by association, it's workforce and trusted data trading partners) will use to implement its overall privacy and security program. This standard requires Covered Entities to;

“Implement policies and procedures to prevent, detect, contain and correct security violations.”

Additionally, the standard lists four required implementation specifications the Covered Entity must account for;

1. Risk Analysis
2. Risk Management
3. Sanction Policy
4. Information System Activity Review

1. Risk Analysis Specification – 45 CFR Section 164.308(a)(1)(ii)(A)

Both Risk Analysis and Risk Management are vital, essential points which form the foundation of how a Covered Entity prepares for and conducts its use and protection of PHI/IIHI/EMR data over time. There is an assessment of readiness and gaps, and establishment corrective actions and ongoing processes to manage the PHI/IIHI/EMR information is handles. It is the process of identifying security risks, and determining the probability of occurrence and magnitude of those risks.

The specification requires the Covered Entity to;

“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”

As the Covered Entity addresses the Risk Analysis Specification, questions it may consider are*;

- How does EPHI flow throughout the organization? This includes EPHI that is created, received, maintained or transmitted by the covered entity.
- What are the less obvious sources of EPHI? Has the organization considered portable devices like PDAs?
- What are the external sources of EPHI? For example, do vendors or consultants create, receive, maintain or transmit EPHI?
- What are the human, natural, and environmental threats to information systems that contain EPHI?

2. Risk Management Specification – 45 CFR 164.308(a)(1)(ii)(B)

The Risk Management Specification requires the Covered Entity to make decisions on how it will address security risks and vulnerabilities with regards to its handling of PHI/IIHI/EMR data. The covered Entity (and its workforce and trusted data trading partners and Business Associates) will want to assure its risk management strategy compliance includes factors found in 45 CFR Section 164.306(b)(2).

As well, the specification requires the Covered Entity to;

“Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR Section 164.306(a).”

As the Covered Entity addresses the Risk Management Specification, questions it may consider are:

- What security measures are already in place to protect EPHI (i.e. safeguards)?
- Is executive leadership and/or management involved in risk management and mitigation decisions?

- Are security processes being communicated throughout the organization?
- Does the covered entity need to engage other resources to assist in risk management?

3. Sanction Policy Specification – 45 CFR Section 164.308(a)(1)(ii)(C)

The Covered Entity's Sanction Policies should be employed with the intent to effectively reinforce its privacy and security procedures. Sanctions for non-compliance must be in place so that;

- workforce members (and trusted data trading partners and Business Associates) understand the consequences of failing to comply with security policies and procedures, and
- as an established means to deter noncompliance.

The specification requires the Covered Entity to;

“Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.”

As the Covered Entity addresses the Sanction Policy Specification, questions it may consider are*;

- Does the covered entity have existing sanction policies and procedures to meet the requirements of this implementation specification?
- If not, can existing sanction policies be modified to include language relating to violations of these policies and procedures?
- Does the organization require employees to sign a statement of adherence to security policy and procedures (e.g., as part of the employee handbook or confidentiality statement) as a prerequisite to employment?
- Does the statement of adherence to security policies and procedures state that the workforce member acknowledges that violations of security policies and procedures may lead to disciplinary action, for example, up to and including termination?
- Does the sanction policy provide examples of potential violations of policy and procedures?
- Does the sanction policy adjust the disciplinary action based on the severity of the violation?

4. Information System Activity Review Specification - 45 CFR Section 164.308(a)(1)(ii)(D)

The Covered Entity's System Activity Review is a set of methodologies used to oversee and account for processes affecting electronic handling of PHI (EPHI). These methodologies, the outcomes from the reports, and the processes and systems covered are part of the Covered Entity's risk management strategy and accountability. And, the State's HIE organization will follow the same approach for its operations, as well as its appropriate oversight of stakeholder participants to the NHIE. The primary goal of this risk mitigation strategy and activity - whether performed individually by any of the stakeholder participants, or coordinated with (or requested by) the NHIE – is to determine if any patient information (PHI/EPHI//IIHI/EMR) is being misused or inappropriately accessed or disclosed in any way.

This specification requires the Covered Entity to;

“Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.”

As the Covered Entity addresses the Information System Activity Review Specification, questions it may consider are;

- What are the audit and activity review functions of the current information systems?
- Are the information systems functions adequately used and monitored to promote continual awareness of information system activity?
- What logs or reports are generated by the information systems?
- Is there a policy that establishes what reviews will be conducted?
- Is there a procedure that describes specifics of the reviews?

2.5.2 Physical Safeguards

Implementing adequate physical safeguards to protect PHI/IIHI/EHR is an essential step to securing the NHIE network, environment, and trust. The steps taken in this regard impact information systems and related equipment and facilities. The Physical Safeguards standards in the Security Rule were developed to accomplish this purpose. As NHIE works with its Governance and Operations organization over the coming months, acquires its HIE technology platform, and begins to build its participant stakeholder base, NHIE will follow the guidelines as set out in the Physical Safeguards Standards.

The Security Rule defines physical safeguards as follows:

“...physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

The Physical Safeguards are another line of defense in addition to the Administrative and Technical Safeguards for protecting PHI/IIHI/EHR. The Covered Entity (and in some cases within the HIE, possibly the Business Associate) must consider all physical access to PHI/IIHI/EHR when planning to address physical safeguards. This may extend outside of an actual office, and could include workforce members’ homes or other physical locations where PHI/IIHI/EHR data is accessible.

The following sections outline the standards as set by the Privacy Rule for Physical Safeguards. NHIE and its Governance and Operations organization, and its HIE technology vendor when selected will implement a HIE system and platform that will support these standards.

Facilities Access Control – 45 CFR Section 164.310(a)(1)

The Facility Access Control standard requires Covered Entities to:

“Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”

A “facility” is defined with three specific components:

- Physical premises
- Interior of building(s)
- Exterior of Building(s)

The Facility Access Control Standard has four implementation specifications. NHIE will require that each NHIE participant follow these specifications.

1. Contingency Operations – 164.310(a)(2)(i)
2. Facility Security Plan – 164.310(a)(2)(ii)
3. Access Control and Validation – 164.310(a)(2)(iii)
4. Maintenance Records – 164.310(a)(2)(iv)

Workstation Use – 45 CFR Section 164.310(b)

The Workstation Use standard requires Covered Entities to specify acceptable and proper use of the electronic computing device(s) that will be used to processing PHI/IIHI/EHR data. This will help minimize any adverse risk that the information being processed across the NHIE might be exposed to. Specifically, the Workstation Use standard requires Covered Entities to:

“Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access PHI/IIHI/EHR”.

This standard must also take into account variants in workforce circumstances and location. Situations like telecommuting, hand-held devices – including mobile devices and smart-phones, must all be accounted for by the Covered Entities as they decide what types of workstation to allow for use in the NHIE.

Workstation Security – 45 CFR 164.310(c)

Workstation Security is a standard that must be applied to fit the specific conditions and needs of a Covered Entity. It is unlikely that all Covered Entities within the NHIE will exist under exactly the same conditions, and with exactly the same functional and security needs for their workstations. Therefore, any risk analysis in this regard must take individual organizational needs into account.

The Workstation Security standard requires the Covered Entity to:

“Implement physical safeguards for all workstations that access electronic PHI/IIHI/EHR so as to restrict access to only authorized users.”

Device and Media Controls – 45 CFR 164.310(d)(1)

This stand is intended to cover any electronic storage device or media that can contain PHI/IIHI/EHR data – and in this case especially as it pertains to the NHIE network. This electronic storage device or media can be:

- any memory device
- hard drive

- thumb drive / flash drive or other removable device
- transportable digital memory
- magnetic tape or tape drive
- optical disk
- any memory card or digital computer memory device of any type

The Device and Media Controls Standard requires a Covered Entity to:

“Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PHI/IIHI/EHR into and out of a facility and the movement of these items within the facility.”

There are four implementation specifications for the Device and Media Controls Standard. These specifications are:

1. Disposal – 164.310(d)(2)(i)
2. Media Re-Use – 164.310(d)(2)(ii)
3. Accountability – 164.310(d)(2)(iii)
4. Data Backup and Storage – 164.310(d)(2)(iv)

2.5.3 Technical Safeguards

Technical Safeguard standards are part of the Security Rule found at 45 CFR Section 164.304. It requires Covered Entities – and in some cases Business Associates possibly when within an HIE environment – to take whatever measure necessary to protect PHI/IIHI/EHR data from internal and external risks.

The Security Rule defines Technical Safeguards as:

“...the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”

The Security Rule also accounts for flexibility, scalability, and technology neutrality. Since at the time of this writing, the NHIE has yet to choose a HIE technology vendor, it will work closely with each NHIE participants and *their* solution vendors to ensure compatibility and compliance with all applicable Technical Safeguards per the Security Rule, so as to be compatible with the NHIE, and therefore with other national standards as well. In addition to using the Technical Safeguard standard and implementation specifications as guidance for all NHIE Covered Entity NHIE participants, NHIE will further publish detailed technical and user manuals, as needed, based on the technology and solutions vendor that NHIE ultimately selects. This vendor and any corresponding technical specifications and user’s manuals will be in place in coordination with the launch of the NHIE.

With regards to the depth, breadth, and extent of the Technical Safeguards a Covered Entity must implement, each organization will be different. Requirements will be different including affordability. And although the

affordability factor could significantly impact a Covered Entity's ability and readiness to participate in the NHIE, the Security Rule does require appropriate levels of compliance with the Technical Safeguards standard.

Access Controls – 45 CFR 164.312(a)(1)

The Access Controls standard covers all aspects of authenticated users of any type of connected, on-line system resource that can grant that user authorized access to PHI/IIHI/EHR. In this discussion, this includes controlled, authorized access to PHI/IIHI/EHR data through the NHIE as well as other Covered Entity systems user access points. These points are also referenced and considered concurrently to 164.308(a)(4) – the Information Access Management rules of the Administrative Safeguards.

The Access Control standard requires a Covered Entity to:

“Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)[Information Access Management].”

The Security Rule does not specify the specific ground rules for Access Control for each Covered Entity – just that each Covered Entity account for adequate access control for their systems and environment. This includes their workforce, and the individual access roles and privileges of each workforce staff. The Director and NHIE will require that the NHIE itself, as well as each NHIE Covered Entity Participant follow and remain compliant with all current Access Control standards.

There are four implementation specifications for the Access Control Standard. These specifications are:

1. Unique User Identification – 164.312(a)(2)(i)
2. Emergency Access Procedures – 164.312(a)(2)(ii)
3. Automatic Logoff – 164.312(a)(2)(iii)
4. Encryption and Decryption – 164.312(a)(2)(iv)

Audit Controls – 45 CFR 164.312(b)

Audit Controls is a standard, like some others, that are very conditional and situational and based on the individual Covered Entity's overall needs. The Director and NHIE will require the NHIE itself as well as all NHIE Covered Entity Participants to comply with an adequate level of audit controls to meet the needs of its own environment and conditions. There are no implementation specifications stipulated by the Security Rule for this reason.

The NHIE and each Covered Entity must consider its own risk factors when building and maintaining its audit controls. These factors should include (but may not be limited to):

- Technical infrastructure
- Hardware security capabilities
- Software security capabilities
- Any other human or information systems security that could impact auditing needs

The Audit Controls standard requires a Covered Entity to:

“Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI/IIHI/EHR data.”

Integrity – 164.312(c)(1)

Ultimately, the primary goal of the Security Rule above all others is to protect the integrity of the PHI/IIHI/EHR data being handled, transmitted and processed – in this case, specifically within the NHIE. A compromise of any data integrity can mean serious consequences in the clinical significance of an individual’s PHI/IIHI/EHR data, adversely and falsely affecting that individual’s data as it is shared throughout the NHIE network. Therefore, it is of absolute importance that the NHIE processes and sharing mechanisms maintain the original meaning and values of all data that passes through the statewide network. For this purpose, integrity is defined as:

“...the property that data or information have not been altered or destroyed in an unauthorized manner...”

As NHIE grows and adds data trading participants to the statewide network, rigorous specifications reviews and adequate integration testing will be performed with each NHIE participant to ensure data integrity is maintained at all times, for the life of the interchange. And, NHIE and all its participants must be accountable for data integrity which can be impacted by:

- Human/work-force factors
- Electronic factors
- Mechanical factors
- Any factor or process within the continuum of care which has the potential to impact data as it is passed from point to point, and trading partner to trading partner

The Integrity standard requires a Covered Entity to:

“Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”

There is one implementation specification for the Integrity standard. This specification is:

1. Mechanism to Authenticate PHI/IIHI/EHR – 164.312(c)(2)

Person or Entity Authentication – 164.312(d)

The primary function of the applied Person or Entry Authentication standard is that within the NHIE and NHIE participant systems, and end user can be identified as a specific individual, and authenticated as a valid user of a given system in order to grant proper access to PHI/IIHI/EHR data. This standard has no set implementation specifications, but is left to the host systems to appropriately handle the conditions it faces within its own environment as well as within the NHIE network adequately identify and authenticate individuals and entities into the system.

The Person or Entity Authentication standard requires a Covered Entity to:

“Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”

Although the NHIE and Covered Entities may employ any number of methods of authentication, some common, basic steps for providing proof of identity can include:

- Require something known only to that individual, such as a password or PIN.
- Require something that individuals possess, such as a smart card, a token, or a key.
- Require something unique to the individual such as a biometric, which could include fingerprints, voice patterns, facial patterns or iris patterns.

Transmission Security – 164.312(e)(1)

The Transmission Security standard requires some analysis, in this case on the part of NHIE and the participating Covered Entities, to determine the types and methods of data transmission that are available for sharing PHI/IIHI/EHR data on the NHIE network. Based on those available methods, be they eMail, internet, or other point-to-point electronic routing, the correct course for maintaining adequate and compliant data transmission security can be determined.

The Transmission Security standard requires a Covered Entity to:

“Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”

There are two implementation specifications for the Transmission Security standard. These specifications are:

1. Integrity Controls – 164.312(e)(2)(i)
2. Encryption – 164.312(e)(2)(ii)

Decryption of Data

Any decryption of data will be handled conditionally based on current technology capabilities of the NHIE and each of the Covered Entities. And ability to decrypt data will go hand-in-hand with the technical ability of the NHIE and its Covered Entities and NHIE participants encrypt data.

3 References & Resources

Supporting reference and resource materials include the following;

1) Health Insurance Portability and Accountability Act (HIPAA)

Specific sections: 164.501, 164.504(e)(2)(i)(F), 164.526, 164.501, 164.520, 164.520(c)(3), 164.304, 164.306(a), 164.306(b), 164.306(b)(2), 164.308, 164.308(a)(1), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B),

- 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(4), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 45 CFR Privacy Rule, 45 CFR Common Rule, 45 CFR 46
- 2) ONC Privacy and Security Tiger Team – various meeting notes and documents available online
- 3) National Institute of Standards and Technology, NIST Special Publication 800-63 Version 1.0.2
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- 4) Health Level Seven (HL7) International
<http://www.hl7.org/Special/committees/visual/index.cfm>
- 5) Nevada Senate Bill No. 43 (SB-43) – Committee on Health and Human Services, Changes Related to Electronic Health Records (BDR 40-443)
<http://leg.state.nv.us/Session/76th2011/Bills/SB/SB43.pdf>
- 6) Office for Civil Rights (OCR) - The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/correction.pdf>
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/opennesstransparency.pdf>
- 7) The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information
<http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cachedtrue&objID=1173>
[http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_18/NationwidePS Framweork-5.pdf](http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_18/NationwidePS_Framweork-5.pdf)
- 8) HHS/CMS HIPAA Security Series #2 - Administrative Safeguards
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf>
- 9) HHS/CMS HIPAA Security Series #3 – Physical Safeguards
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf>
- 10) HHS/CMS HIPAA Security Series #4 – Technical Safeguards
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>